REMARKS

Claim Changes

Claim 1 has been amended to more clearly recite the claimed invention. Particularly, independent claim 1 has been amended to recite "An asymmetric cryptographic processing system using a multiple key hierarchy, the asymmetric cryptographic processing system comprising: a digital processing device; a first key for performing asymmetric operations at a first rate in the digital processing device, wherein each operation requires a first cryptographic processing time; and a second key for performing an asymmetric cryptographic processing operation in the digital processing device to update the first key, wherein the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate and that requires a second cryptographic processing time greater than the first cryptographic processing time." Independent claim 16 has been amended to recite similar subject matter to claim 1. No new matter is added by the amendments.

No amendment made is related to the statutory requirements of patentability unless expressly stated herein. No amendment is made for the purpose of narrowing the scope of any claim, unless Applicant had argued herein that such amendment is made to distinguish over a particular reference or combination of references. Any remarks made herein with respect to a given claim or amendment is intended only in the context of that specific claim or amendment, and should not be applied to other claims, amendments, or aspects of Applicant's invention.

Rejection of claims 1-7 and 16-19 under 35 U.S.C. § 101

Claims 1-7 and 16-19 are rejected under 35 U.S.C. § 101. Claims 1 and 16 have been amended to recite a digital processing device. Applicant respectfully submits that as amended, claims 1 and 16, and their dependent claims 2-7 and 17-19, more clearly recite statutory subject matter. Accordingly, Applicant respectfully requests the rejection be withdrawn.

Rejection of Claims 1-7 and 10-15 under 35 U.S.C. § 103(a) as being unpatentable over "Handbook of Applied Cryptography" (Menezes) in view of US 6044350 (Weiant)

Applicant respectfully traverses the rejection of claims 1-7 and 10-15. Reconsideration is respectfully requested.

The present invention uses multiple public/private key pairs of varying levels of security. The lower-security level includes keys which are small in length, which are changed relatively often, and which require low resources to implement their coding functions. When it is desired to change key pairs of low security, a key pair at a higher security level (i.e., longer length keys) than the lower-security level keys is used to transfer the new lower-security public keys to devices using the higher-security keys. The higher security keys can, in turn, be changed at a frequency lower than the lower security keys. The higher-security keys require a higher level of resources to perform their coding operations. This approach of using keys of escalating levels of security to replace lower-security keys, where the higher-security keys require more resources, are more secure, and are replaced less often than the lower-security keys, can be followed as many times as is desired to create a hierarchy of public key uses with the result that the lower-security operations can be performed quickly while the overall system security is high.

The Office Action on page 4 states "Menezes et al. does not specifically teach the second key requires a second cryptographic processing time greater than the first cryptographic processing time. Weiant, Jr. et al. teaches the second key requires a second cryptographic processing time greater than the first cryptographic processing time (fig. 3)."

Applicant respectfully submits that the combination of Menezes and Weiant does not teach or suggest all the claim limitations as set forth in independent claims 1 and 10. For example, independent claim 1 recites "the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate and *that requires a second cryptographic processing time greater than the first cryptographic processing time*" which is not taught or suggested in the combination of Menezes and Weiant. Independent claim 10 recites similar subject matter.

Weiant is directed towards a system for providing the user with the capability of selecting one of a plurality of different indemnification provisions for a particular signed message issued by a certificate meter. See Weiant, Abstract. Menezes discloses a key layering

technique for distributing cryptographic keys when confidentiality of the private and symmetric keys must be preserved. The key layering technique consists of master keys at the highest level, key-encrypting keys, and data keys, wherein the data keys are used to perform cryptographic operations on user data and the key-encrypting keys are encryption public keys used for key transport or storage of other keys.

Weiant in figure 3 merely illustrates a table that describes an association between different keys having different lengths and different processing times. Applicant respectfully submits that the Weiant reference fails to disclose or suggest that one of these keys, described in the table, is a session or key-registration key. Moreover, Weiant also does not disclose or suggest that a session key (or data key) or a key encryption key (or transport key) is of any particular length.

Menezes also fails to disclose or suggest that the session keys have a higher or lower number of bits, as compared to a key-encrypting key. The Menezes reference does in fact describe layering of public key approaches to encryption, but does not describe the higher layer (key-encrypting keys) as necessarily being or using longer and/or slower public keys.

The Office Action on page 11, item 7, states:

> Applicant previously argued that Menezes discloses the time period (long-term and short-term) over which the data key is valid, and not the rate (frequent or infrequent use) at which the data key is used for performing asymmetric operations. Menezes does mention the data keys being a short-term key and the key-encrypting keys as being long-term keys, which means the data keys are only meant to last a short time compared to the key-encrypting keys. However, Menezes also mentions that the data keys are session keys (see page 553, section 13.10, short-term keys). Session keys are used repeatedly during an entire session, and then they are updated for the start of a new session. The rate at which the session key is used is much higher than the keys used to update the session key.

The Examiner cites no support from Menezes for the contentions that "[s]ession keys are used repeatedly during an entire session, and then they are updated for the start of a new session" and that "[t]he rate at which the session key is used is much higher than the keys used to update the session key." Applicant respectfully traverses the Examiner's unsupported statements.

It is respectfully submitted there is no motivation or suggestion in either the Menezes or Weiant references that would motivate a person with ordinary skill in the art to believe that the length of the session keys would be either longer or shorter than those of the key-registration keys. Thus, there is no teaching or motivation in either of these references that suggests or

describes that the processing with either of the two keys will take longer than the other. Therefore, Applicant respectfully submits that the combination of Menezes and Weiant does not suggest or describe "the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate and *that requires a second cryptographic processing time greater than the first cryptographic processing time*" as recited by independent claim 1. Independent claim 10 describes similar subject matter.

Dependent claims 2-7 and 11-15 depend from, and include all the limitations of independent claims 1 and 10. Therefore, Applicant respectfully requests the reconsideration of dependent claims 2-7 and 11-15 and requests withdrawal of the rejection.

For at least the above reasons, Applicant submits that claims 1-7 and 10-15 are not obvious in view of the combination of Menezes and Weiant, and therefore that the rejection of claims 1-7 and 10-15 under 35 U.S.C. § 103(a) should be withdrawn. Applicant requests that claims1-7 and 10-15 now be passed to allowance.

Rejection of Claims 16-19 under 35 U.S.C. § 103(a) as being unpatentable over US 5850443 (Van Oorschot) in view of "Handbook of Applied Cryptography" (Menezes)

In view of the above explanation with respect to independent claim 1, Applicant respectfully submits that Menezes fails to describe or suggest "wherein the second length is longer than the first length, further wherein the first key encryption processing operations is at a second rate that is less often than the first rate and *that requires a second cryptographic processing time greater than the first cryptographic processing time*" as recited by independent claim 16, as amended. Moreover, Van Oorschot fails to remedy the acknowledged deficiency of Menezes.

Dependent claims 17-19 depend from, and include all the limitations of independent claim 16. Therefore, Applicant respectfully requests the reconsideration of dependent claims 17-19 and requests withdrawal of the rejection.

Conclusion

Applicant respectfully submits that Applicant's claimed invention is patentably distinct and nonobvious over each reference taken alone or in combination, and requests that a timely Notice of Allowance be issued in this case. Should the Examiner have any questions, comments, or suggestions, the Examiner is invited to contact the Applicant's undersigned attorney at the telephone number indicated below.

Please charge any fees that may be due to Deposit Account 502117, Motorola, Inc.

Respectfully submitted,

ERIC J. SPRUNK, et al.

Date: March 16, 2010

By: /Stewart M. Wiener/

Stewart M. Wiener
Attorney for Applicant
Registration No. 46,201
Tel. No. (215) 323-1811
Fax No. (215) 323-1300

MOTOROLA, INC.
101 Tournament Drive
Horsham, PA 19044